REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority: N/A

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol:
C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):
Key Vulnerability: Seaports of Embarkation

9. Personal Authors:
LCDR Anthony T. Calandra

10.Type of Report: FINAL

11. Date of Report: 03 Feb 2003

12.Page Count: 17 **12A Paper Advisor (if any):**

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: Embarkation, Port Security, Chemical/biological attacks, terrorist attacks, logistics, force protection, Seaports, Homeland Security, Deployment, military transportation

15.Abstract:

Recent asymmetrical attacks on U.S. soil have driven home the fact that a significant threat exists inside the borders of this country. This, coupled with the current limitations on seaport embarkation infrastructure and logistical capability, gives rise to a new vulnerability to the United States military: The threat of an asymmetrical attack on deploying forces at a seaport of embarkation. Such an attack would reduce the number of forces available to the Operational Commander awaiting these forces and could also lead to a significant delay in the arrival of assets due to the loss transportation equipment of access to contaminate ports of embarkation. The current system to defend against such an attack is unsatisfactory. A proper joint doctrine focused on defining specific responsibilities and based upon deterrence must be established to ensure the security of deploying forces and to best support the Operational Commander.

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-3556

20.Office Symbol: **C**

Security Classification of This Page Unclassified

NAVAL WAR COLLEGE
Newport, RI.

Key Vulnerability: Seaports of Embarkation

by

Anthony T. Calandra

LCDR USN

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College of the Department of the Navy.

Signature: _____

03 February 2003

ABSTRACT

Key Vulnerability: Seaports of Embarkation

Recent asymmetrical attacks on U.S. soil have driven home the fact that a significant threat exists inside the borders of this country. This, coupled with the current limitations on seaport embarkation infrastructure and logistical capability, gives rise to a new vulnerability to the United States military: The threat of an asymmetrical attack on deploying forces at a seaport of embarkation. Such an attack would reduce the number of forces available to the Operational Commander awaiting these forces and could also lead to a significant delay in the arrival of assets due to the loss transportation equipment of access to contaminated ports of embarkation. The current system to defend against such an attack is unsatisfactory. A proper joint doctrine focused on defining specific responsibilities and based upon deterrence must be established to ensure the security of deploying forces and to best support the Operational Commander.

Table of Contents

INTRODUCTION:

At 0130 hours, three Marines decided it was time to return to their quarters at Camp Lejeune and rest before the next day's deployment. They had enjoyed their last night of "freedom" on American soil before a long awaited combat deployment. What they did not know was that one of the “locals” had been planning the evening’s events for months. What looked like a simple offer to buy a round of beer was actually a devastating, asymmetrical attack. As they drank a round on the stranger, each Marine was infected with a highly contagious and deadly disease. Simultaneously, a small group of this terrorist’s associates was conducting an attack on military vehicles loaded on a nearby freight train. The men pulled off the road that paralleled the Beaufort - Morehead City rail line and sprayed a liquid onto the handrails and controls of several military vehicles loaded on the train. A third group of terrorists was preparing for a more direct attack on embarkation operations at the port of Morehead City the following day. Their plan was simple - a small truck, a dirty bomb and a willingness to die for their cause.

The embarkation proceeded smoothly until 1330 hours when a large commotion occurred at a security gate. Tires squealed, there was a crash and shots were fired. Sirens followed a brief moment of silence as emergency vehicles raced toward the gate. A direct attack by three armed men had narrowly been avoided. After a short evacuation, things returned to normal and the three Marines boarded the large gray ship that would be their home for the next two weeks.

Four days into their journey, the ship transmitted a flash message issuing the news. Something was terribly wrong onboard the amphibious vessel. Men were critically ill and the

sickness was spreading like wildfire. The ship had to return to port and the Operational Commander had lost a valuable asset before battlefield hostilities had ever begun.

This is not a segment from a Tom Clancy novel, nor is it a lead-in for a Hollywood movie; it is a major, real world problem. Unfortunately, in spite of the increased emphasis on homeland security, the vulnerability of U.S. port facilities and embarking forces is closer to reality than fiction. U.S. military forces are ill-equipped and ill-supported to counter or successfully manage a chemical or biological attack while conducting embarkation operations within the United States. Port security measures are often developed ad-hoc and rarely conform to any formal doctrine. In order to properly support the Operational Commander a concise, structured, joint doctrine, focused on deterrence, should be developed to prevent unconventional / asymmetrical attacks from impeding deployment efforts.

While the current security posture within the United States has improved since September 11, 2001, there are still major shortfalls that create significant hazards to deploying forces. "Ports are inherently vulnerable to terrorist attacks because of their size, generally open accessibility by water and land, location in metropolitan areas, the amount of material being transported through ports, and the ready transportation links to many locations within our (U.S.) boarders."[1] The current shortfalls in port security are a result of insufficient funding, disorganization and poor interagency cooperation. While there has been a significant increase in the number of agencies supporting the effort to improve homeland security and more specifically, seaport security, little has been done to improve the larger process or establish clear lines of responsibility. If embarking forces were limited to military ports, the problem would be simple. But due to constraints on infrastructure, most embarkation operations occur

alongside commercial port activities. This complex issue requires different levels of security for different operations.

CURRENT EMBARKATION SECURITY CRISIS:

Most ports cater to multiple users and stretch over large geographical areas. Because of the need to move large amounts of material, access must be simple and efficient. If the movement of goods is slowed for any reason, efficiency and commercial profitability are sacrificed. Ownership, location, size, access and a variety of users all combine to complicate how responsibility for security should be levied. Under funded agencies with overlapping responsibilities make the problem even more difficult. Unfortunately, the establishment of additional governmental and military organizations has only further confused the issue of port security. A partial list of agencies currently involved in the security of embarkation procedures include: The Department of Transportation, U.S. Coast Guard, U.S. Transportation Command, CIA and FBI, U.S. Navy, INS and Customs Departments, local and state police forces, port owners, private civilian security companies and most recently, the Department of Homeland Security and U.S. Northern Command. This mass of organizations and a lack of clearly defined responsibilities hamper efficiency and security. Understanding who is in charge or the central point of contact is often confusing. These problems and the lack of interagency cooperation are due mainly to an absence of structure and organization.

PITFALLS OF THE DECONTAMINATION STRATEGY:

A chemical or biological attack on a U.S. port embarking military personnel could spell disaster for an Operational Commander's war plans. Even if the attack was limited in scope and with few fatalities, the decontamination process could have a greater impact than the attack. Decontamination takes time, labor and space. As an example, the effort required to

decontaminate one M1-A2 Abrams tank includes approximately one and a half hours (not including decontamination station set up time) 15 gallons of decontaminate, and nearly 400 gallons of water.[2] This time delay is unacceptable for the Operational Commander. Removing just one ship and its cargo for a limited amount of time would produce a ripple effect that could significantly degrade the combat capability of a force in theater. As the U.S. Armed Forces continue to stress logistical assets to the limit and rely on "just in time" supply and deployment principles, the effects of a Nuclear/Biological/Chemical, (NBC) attack on embarking forces become overwhelming. Additionally, due to the current limited capabilities of decontamination equipment and procedures, there would be some permanent loss in personnel and equipment. Rubber, canvas and cloth are particularly susceptible to loss due to the embedding of contaminate. Electronics and optics can be severely damaged by the corrosive nature of the decontamination chemical.[3]

Decontamination requires both time and money and is not always effective. The best-case scenario is to avoid an attack all together. The three tenets to NBC defense are: 1) Contamination avoidance, 2) Protection of units and personnel, and 3) Decontamination.[4] Of these three, avoidance is the key to successful embarkation operations. The benefits of avoiding an NBC attack are well worth the effort and include:

1. Avoiding casualties to both personnel and equipment.
2. Upholding the schedule of the embarkation process and preserving Time Phased Force Deployment Data (TPFDD) requirements.
3. Maintaining viable port facilities for both military and commercial operations.
4. Protecting the local populous from the fallout of an attack.

Most importantly, avoidance best supports the Operational Commander by providing the resources required to conduct the mission on the required and planned timeline.

THE STRATEGY OF DETERRENCE:

While deterrence represents the most advantageous form of combating NBC attacks on embarking forces, it also requires the most robust and sustained commitment of effort. Deterrence can be achieved in several ways. First, the threat of punishment can make the consequences of such an attack so severe that its costs outweigh its benefits. In a similar type of asymmetrical attack against the World Trade Center on September 11, 2001, the United States responded by attacking the perpetrators and their host nation of Afghanistan. The long-term effects of such a punishing retaliation have yet to be determined, but it can certainly be argued that other terrorist groups and host nations must now calculate the response the United States will take against similar attacks. For this type of deterrence to be effective, the attacker must feel that the threat posed to him is credible and exceeds his acceptable cost-benefit ratio.[5] The retaliatory strikes against Al Quada and the Talliban gave this type of deterrence credibility, but any lapse in U.S. response to similar asymmetrical attacks erode that credibility. Such deterrence is not cheap. To date operation ENDURING FREEDOM has cost the United States $10.1 billion.[6] Even if combat operations are not required, offensive forces must be maintained in order to maintain the credibility of retaliation.

Deterrence can also come in the form of denial. The strategy is to convince the attacker that an NBC defense can successfully counter such attacks, pushing the effort beyond acceptable cost-benefit ratios. Denial can be accomplished passively by mitigating the effects of an attack though defensive preparation or actively by denying use of delivery platforms or developing an impermeable perimeter defense.[7]

Other measures used to mitigate the effects of an NBC attack can involve vaccination programs, protective clothing, masks, hardening vehicles and equipment and the use of

decontamination equipment. Programs such as these, while crucial to the NBC defense of any military force, are expensive, cumbersome and not always 100 percent effective. They can however, reduce the effectiveness of an attack to the point at which one could be convinced that an attack is not worth the costs involved.[8]

Defensive perimeters can take on many forms, the broadest being the worldwide limiting of weapons of mass destruction proliferation and transportation. The next layer in denial would be the security of the nation's outermost borders, while the innermost layer is the protected facility itself. For most seaports of embarkation, the two inner layers are coincident. This, in essence, removes one layer of defense. While the innermost perimeter is potentially the most cost effective way of protecting embarking forces, a more complex, virtual perimeter must also be developed around the personnel and equipment to protect against attacks prior to staging at the embarkation port.

A third type of deterrence is often forgotten due to its non-military nature. This is the act of preventing the asymmetrical attacks of an organization by removing its reason for attack. Obviously, this should only be attempted if the agenda is legal and moral, and should not be attempted after a violent attack has occurred. There is a significant cost-benefit advantage, however, to eliminating the reasons behind violence before it occurs. Developing an active program to better forecast radical movements and remove their motivation through peaceful conflict resolution would be resources well spent. Although this tactic would not be applicable to all situations and would never completely negate the threat of an asymmetrical attack against the U.S. homeland, it could greatly reduce the exposure to the threat. Had the terrorists in the opening scenario been approached before they resorted to violence, some of their grievances may have been resolved. Better execution and explanation of U.S. foreign policy may be all

that is required to defuse some radical movements. But, as the scenario and recent events point out, there are numerous individuals and organizations that are willing to resort to extreme measures. While this type of deterrence remains an important avenue the United States must address, current events have revealed that this will never be a complete solution. President Bush has pointed out that, evil does exist in this world, and as former President Clinton said, "The U.S. must be prepared to fight and win where asymmetrical means are used against us."[9] The threat to embarking forces is credible and must be addressed in order to fulfill the obligations to the Operational Commanders.

THE REQUIREMENT FOR DOCTRINE:

In order to adequately protect seaports of embarkation, a standard joint doctrine including all deterrence methods must be developed. This doctrine must bridge the gaps between all agencies both internal and external to the Department of Defense. Although each of the country's 19 major seaports of embarkation vary significantly in structure, access, mission and landscape, the doctrine must be specific enough to provide a repeatable framework for securing the port and its contents. Simultaneously, the policy must not be so overbearing as to impede those modifications required for each facility. The doctrine should include different stages of protection to allow for the efficient flow of commercial goods during times of low threat and extra protection during elevated threat conditions. Duplication of effort and unnecessary bureaucracy must be eliminated while the transfer of vital information between agencies must be streamlined. In order to work properly, this doctrine should contain ten key elements:

1) Assignment of primary agencies responsible for seaport security.
2) Development of a repeatable tiered port security structure.
3) Assignment of a responsible agency for added security forces when required.

4) Identification of organizations responsible for the safety of deploying forces from home station to the actual vehicle used to transport them into theater.

5) Identification of those agencies responsible for supporting the primary security agencies with intelligence and threat information.

6) Identification of a lead agency to ensure overall national security, interagency cooperation and oversight authority with power to levee penalties for security violations.

7) Development of a conduit between each supporting agency and the primary security agencies to pass vital information quickly and accurately

8) Funding for equipment and training to identify and neutralize NBC attacks.

9) A means for the Operational Commander, Captain of the Port and all other organizations involved to provide feedback to the lead agency for process improvement.

10) Support through other measures of national deterrence.

PORT OF EMBARKATION SECURITY IMPLEMENTATION:

Currently, each major seaport of embarkation has its own security program. One thing common to each, however, is the Captain of the Port. This is normally a Coast Guard Captain who is very knowledgeable and well trained but ill-equipped. In fact, most Captains of the Port have no indigenous assets assigned to them. This lack of assets is normally offset slightly by the security provided by local and state law enforcement or private security companies hired by the owner/operators of the port.[10]

The requirement at this most basic level of seaport security should be a well-organized, tiered security doctrine under the local control and responsibility of the Captain of the Port. This doctrine would be repeatable in each major seaport and could be an example from which other major assets within the United States are secured. The program would contain varying security measures for different DHS threat levels, intelligence data and the specific operations currently being conducted at the port.

For the doctrine to be successful, the shortfalls currently experienced by the Captain of the Port would have to be rectified. He must have at his disposal the equipment and infrastructure required to adequately conduct his mission. The Coast Guard's role and responsibilities would increase substantially, its procurement and operating budget would have to be increased as well. But according to this doctrine, the Coast Guard would not be the sole provider for security at all DHS threat levels.

For more germane situations and operations, much of the Captain of the Port's equipment would remain on standby as local law enforcement and civilian security companies would share the burden. At times of increased threat levels, the Captain would integrate more of his own resources and, as required, receive additional help from outside agencies. An example of this would be during the actual embarkation of combat forces. For embarkations, U.S. TRANSCOM, more specifically, Military Traffic Management Command, (MTMC) in addition to the actual deploying units would supplement port security.

To some, the selection of MTMC may seem to miss the mark, but examining their mission and capabilities makes the selection quite clear. "Throughout the world, MTMC coordinates force movements to seaports, prepares the seaports for ships and cargo, and supervises loading/unloading operations."[11] Additionally, it can monitor port status and infrastructure on a worldwide basis. MTMC can also provide the manifest documentation and tracking services that are key to ensuring the security of shipped goods.[12] With modest increase in resources, this command could provide a much-needed boost to port security.

MTMC's major role would be to provide logistical information necessary to facilitate proper security measures. Through the establishment of force protection teams, complete with defensive capabilities, MTMC could also provide defensive support to those units unable to

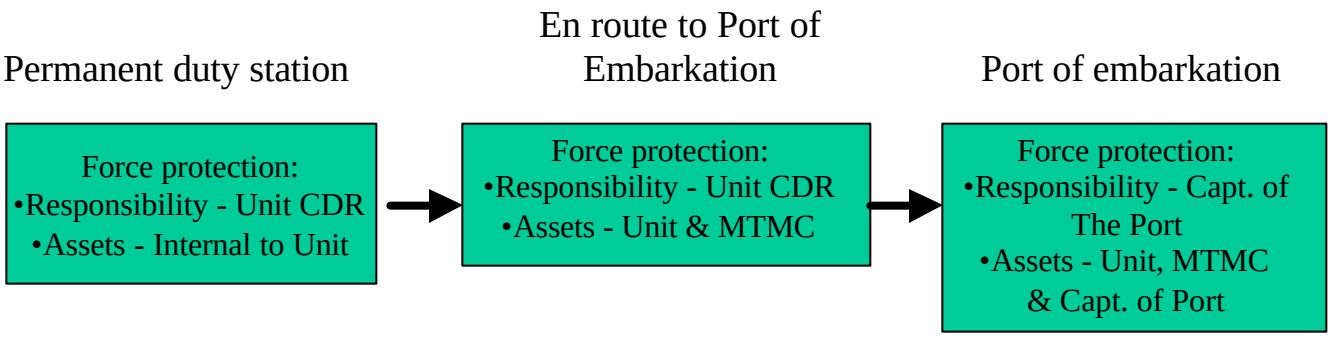
fulfill their own force protection requirements. The deploying forces themselves could provide significant force protection during embarkation operations. Through very minor adjustments to deployment procedures, each unit could provide protection to its personnel and equipment during the movement to the embarkation facility and during the staging and loading process. In the opening scenario, had MTMC and the deploying units been working together, they could have identified the key areas of vulnerability for the equipment being deployed and provided adequate security to keep that equipment from being contaminated.

Under this doctrine, once a unit leaves its home station for deployment, the ultimate responsibility for the unit's force protection will remain internal to that unit. The unit will be assisted, however, by MTMC, and the level of involvement will vary according to individual unit requirements.

Force protection must include close and constant monitoring of all deploying equipment and additional protective measures for personnel. Deploying service members should be medically screened prior to deployment and quarantined during the final 24 hours prior to embarking. Outside of the 24-hour window, monitoring systems available to detect chemical and biological contaminants will protect the forces. Currently, it takes a maximum of 24 hours for the monitoring equipment to determine if exposure has taken place. Personnel exposed to contamination outside the 24-hour containment window would know of their status due to the results of tests from the local monitoring devices (current technology requires approximately 24 hours to analyze test samples) or the presence of symptoms associated with a chem/bio agent. [13,14]

Once the unit arrives at the port of embarkation, force protection will be the primary responsibility of the Captain of the Port. MTMC and the deploying units would continue to

provide force protection services under the direction of the Captain of the Port. The Captain of the Port would maintain overall operational control and responsibility for the safety of forces inside the port's perimeter. A tiered approach to security based upon the current threat level would allow for increased port efficiency during times of reduced threat, and save the cost of continually operating security forces at heightened levels.



For this procedure to function properly informed decisions based upon valid information must be made. Responsibility for assigning threat levels to ports of embarkation would fall to the Captain of the Port. For the Captain to make the proper decision, he must have proper and timely information. For the doctrine to work properly, the Captain must receive adequate intelligence information from supporting agencies such as the FBI, CIA and NSA. This will necessitate the requirement for handling classified material, possibly at the top-secret level. While the Captain of the Port's staff is well trained in port security and Coast Guard operations, it will need additional training, manning, equipment and possibly upgraded security clearances to process this information.

The importance of correctly categorizing threat levels cannot be overstated. Security levels will directly affect the commercial operation of the port. Despite the best efforts in establishing the outer layers of deterrence mentioned earlier, it cannot be guaranteed that each of the nearly 6 million shipping containers[15] that arrive annually in U.S. ports is safe. If

security dictates, the Captain of the Port will have the authority and responsibility to halt commercial operations and establish quarantine areas.

In order to perform efficiently, the Captain of the Port should not be tasked to deal with these information assets directly. The information and intelligence should be filtered through an agency developed to conduct such an effort. The establishment of such a conduit would ensure that the Captain is being supported with properly filtered information from the support agencies. This responsibility must reside with a department that has control over both the Coast Guard and the supporting agencies.[16] This should be one of the primary duties for the new Department of Homeland Security (DHS). Under this doctrine, DHS will also be required to provide a structure by which critical intelligence information is efficiently channeled to the right people. In the opening scenario, had the Captain of the Port been informed of the heightened level of terrorist activity in the region, he would have been better prepared to prevent or halt a direct attack. The Department of Homeland Security's mission statement; "To prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism; and minimize the damage and recover from attacks that do occur"[17] supports this role. When examining the proposed organizational structure of this new department, its role in seaport security becomes even more significant. Each of its four divisions: Border and transportation security, emergency preparedness and response; chemical, biological, radiological and nuclear countermeasures; and information analysis and infrastructure protection all help identify or control the threat to ports of embarkation and support the Captain of the Port.

The DHS must also provide a system by which ports of embarkation can be evaluated on their security procedures and, if applicable, be able to reprimand those sites that are not

providing the required measures. Other agencies must also be monitored for proper support to the Captain of the Port.

The DHS is also the agency best suited to manage the funding required to keep each phase of this future doctrine functioning properly. The equipment and intelligence necessary to carry out this doctrine is available. Procurement and distribution of resources is the challenge to making this doctrine function properly. The DHS in conjunction with the DOD will have the capability to see that this important aspect of security is managed properly.

Finally, a feedback process must be developed to ensure that no aspect of this complicated security challenge is overlooked. Every new doctrine, program or idea must include a method by which progressive ideas as well as unforeseen shortfalls can be addressed. Because it is the dominant agency in this doctrine, the Department of Homeland Security must support this feedback system.

COUNTER ARGUMENTS:

Opponents to this course of action will quickly point out that it is unethical not to provide adequate defense from a NBC attack through a robust decontamination program. The proposed concept does not preclude the use of decontamination procedures, nor does it reduce the current inventory of equipment available for the task. The ability to decontaminate personnel and equipment is an essential part of deterrence. This doctrine states that attacks must be prevented to best support the Operational Commander. If an attack occurs and decontamination procedures are successful, the unit is spared but the Operational Commander still fails to obtain those forces on time. The current deployment structure of the U.S. military and its ever-increasing areas of responsibility tax TRANSCOM's assets to near capacity. In many TPFDD scenarios, the loss of a single transport vessel can cause huge and sometimes

uncontrollable ripple effects that can lead to significant shortfalls on the Operational Commander's list of required forces.

An additional counter-argument to this doctrine is the lack of use of National Guard units to conduct major security operations inside U.S. borders. While on the surface this would seem to be a logical practice, historical data and current events delineate a significant limitation to the use of the National Guard. The mission of the National Guard is to "maintain properly trained and equipped units, available for prompt mobilization for war, national emergency, or as otherwise needed."[18] Guard units normally carry out this mission as part of the deployed forces. In the last three major U.S. campaigns, a significant number of National Guard units performed their duties well outside the borders of the United States. In fiscal year 2001, Army National Guard soldiers served in more than 80 countries in a wide variety of operations. The Army National Guard alone provides over 36 percent of the regular forces Combat Support force structure. [19] A call to the National Guard to provide port security during a major deployment would most likely go unanswered due to the fact that so many units would already be forward deployed. While some believe that the Department of Homeland Security will push for an end to the use of National Guard units to supplement their active duty service member counterparts, the fact remains that the U.S. military would have a very difficult time projecting significant power without a replacement for the lost assets of the National Guard. Consequently, until there is a replacement force to fulfill the in-theater missions carried out by the National Guard, their domestic use during times of armed conflict will be limited.

A further argument against the proposed plan for protecting embarking forces involves using regular military forces assigned to the newly established U.S. Northern Command. However, a close examination of U.S. Northern Command's mission and structure reveals why

this would be a poor choice. Northern Command's mission is "homeland defense and civil support."[20] It is tasked with conducting homeland defense, the protection of the U.S. against attacks from outside the United States. This is not synonymous with homeland security, the prevention and deterrence of aggression, a subtle difference that Northern Command finds important to delineate. Prevention and deterrence are exactly what is required to ensure that deploying forces are not subjected to attack, which would preclude their timely use. In addition to this dichotomy of mission, U.S. Northern Command has no permanent forces assigned for a continuous mission. Finally, there are specific laws such as the Posse Comitatus act that prohibit the direct use of the military in a law enforcement role on U.S. soil.[21] These restrictions make Northern Command a poor choice for the defense of ports of embarkation.

Some point directly to the newly established Department of Homeland Security to provide U.S. port security. Their argument is that this new department is specifically tasked to provide port security to the country. There is no real argument against this idea. The Department's stated mission completely supports the idea of protecting major seaports and other critical infrastructure within U.S. borders. Many of its initiatives, such as the creation of "Smart Boarders" to stop terrorist from entering the country and the increased security of international shipping containers significantly reduce the threat to deploying forces in ports of embarkation.[22] The establishment of new federal agencies alone, however, will not solve security issues. The development of significant detailed plans at the operational level to support the Department to ensure port security during all operations must be accomplished.

CONCLUSION:

Since the recognition of the fact that the United States is vulnerable to an asymmetric attack within its political borders, there have been significant proposals to change the way

forces are used to protect the homeland. Unfortunately, many of these proposals are too broad in focus to actually lead to improvement in port security. It cannot be argued that the proper framework must be established from the highest echelons of government to ensure national security. But when addressing matters as specific as the security of ports of embarkation for U.S. military forces, a much more detailed plan with specific personnel assigned specific responsibilities is required. It is unfortunate that the United States military lacks the ability to move significant combat forces from U.S. bases into foreign theaters without passing through the same ports used by the commercial transportation industry. Because of this interaction, security must involve not only the Department of Defense, but also local, state and federal agencies. The only way to efficiently integrate the assets of each organization and optimize their involvement is through the development of a solid doctrine developed and understood by all involved parties. Lack of depth in both combat forces and in transportation assets forces the United States to eliminate as much risk as possible to ensure the Operational Commander has the assets necessary to carry out his assigned tasks. Current planning does not compensate for the closure of major ports of embarkation or even the loss of a small amount of transportation assets. Embarking U.S. forces must be protected with the same enthusiasm and effort as when they are at their home station or debarking within the theater. In order for this protection to become a reality, a specific joint doctrine, which includes not only military forces, but also local and state law enforcement as well as other federal agencies must be established, organized and properly funded. There must be a chain of responsibility established from the time a deploying unit leaves the confines of its base until it is safely en route to the theater.

Upon notification of deployment, individual units must ensure their own security from their base to the port of embarkation. With assistance from MTMC, a detailed plan must be

developed to establish the modes of transportation, identify areas of significant risk and ensure robust accountability for the security of each individual and piece of equipment.

Because of its unique mission, training, capabilities and experience, the Coast Guard's Captain of the Port must be at the center of effort to ensure the port and the material staged for embarkation is safe from attack from air, land and sea. To enable him to complete his task, he must have the direct assistance of the deploying units; U.S. MTMC; private, local, state and federal law enforcement as well as those other agencies under the coordination of the Department of Homeland Security. Additionally, the DHS (via the FBI and other agencies) must supply the Captain of the Port with intelligence and specific indications and warnings in order to properly identify the level of threat. Through a tiered security approach involving the entire port complex, the Captain of the Port can protect both the deploying forces and the commercial and civil interests in his area of responsibility.

This type of doctrine is dependent on proper funding and allocation of assets. Through the Department of Homeland Security, there is already a significant increase in the budget for the Coast Guard due to its increasing roles in homeland defense. This proposal will require an additional allocation of funds and resources in order to be effective. In addition to monetary and physical resources, information and intelligence resources must also be increased to ensure those responsible for protecting deploying forces have the resources to complete the mission.

Failure to establish a more robust security plan for seaports of embarkation is a risk that the United States cannot afford to. Placing the Operational Commander in a situation where he may not have the required assets available to carry out his mission would be unforgivable. Although the cost to implement this doctrine will be significant, it is an efficient and effective way to ensure U.S. military power is deployable.

ENDNOTES

[1] JayEtta Z. Hecker, "Statement," U.S. General Accounting Office, Subcommittee on National Security, Veterans Affairs, and International Relations House Committee on Government Reform, Port Security, Nation Faces Formidable Challenges in Making new Initiatives Successful, GAO-02-993T, 5 August 2002, 2.

[2] Army Department, NBC Decontamination, FM 3-5 (Washington, DC: 2000), 4-20, 4-21.

[3] Ibid, 5-8.

[4] Greg D. Olson, "Operational Concerns of Decontamination in Mitigating the Effects of Chemical and Biological Weapons Against Sea Ports," (Unpublished Research Paper, U.S. Naval War Command and Staff College. Newport, RI: 13 May 2002), 2.

[5] Keith B. Payne, "Deterring the Use of Weapons of Mass Destruction: Lessons from History," Comparative Strategy, Vol. 14 No. 4, (October 1995): 349.

[6] Mike Lofgren, "Measuring the Cost of the War Against Terrorism," The Budget Defense Monitor, 19 June 2002, Vol. 2, No 6, <http://www.budget.house.gov/budmon2006.pdf> [28 September 2001], 2.

[7] Payne, 354.

[8] Payne, 347, 350.

[9] William J. Clinton, A National Security Strategy for a Global Age, The White House, Washington, DC, (December 2000), 11.

[10] James F. Murray, U.S. Coast Guard Group Commander, telephone conversation, 22 January 2003.

[11] Transportation Command, Understanding the Defense Transportation System, USTRANSCOM Handbook 24-2, third edition, (Washington DC: 01 September 2000), 10.

[12] Ibid, 9.

[13] Judith Miller, "U.S. is Deploying a Monitor System for Germ Attacks," The New York Times, 22 January 2003, sec. A, p.1.

[14] Frederick Sidell, Ernest T. Takafuji and David R. Franz, Medical Aspects of Chemical and Biological Warfare, Borden Institute, Walter Reed Army Medical Center (Washington, DC: 1997), 546.

[15] JayEtta Z. Hecker, 3.

[16] While not all supporting agencies fall under the DHS, it is expected that they will provide support to this department.

[17] "The Department of Homeland Security," The White House Home Page, <http://www.whitehouse.gov/deptofhomeland/> [24 January 2003], 1.

[18] "Aiding America's Communities, Our State Mission," The Army National Guard Homepage, <http://www.arng.army.mil/about_us/ai ding_america.asp> [31 January 2003], 1.

[19] Ibid

[20] "Who We Are -- Mission," U.S. Northern Command Homepage, <http://www.northcom.mil/index.cfm?fuseaction=s.whoweare&section=3> [20 December 2002], 1.

[21] "Homeland Defense," U.S. Northern Command Homepage, <http://www.northcom.mil/index.cmf?fuseaction=s.homeland> [20 December 2002], 1.

[22] Office of Homeland Security, The National Strategy for Homeland Security, Washington, DC: 16 July, 2002, 60.

SELECTED BIBLIOGRAPHY

"Aiding America's Communities, Our State Mission." The Army National Guard Homepage. <http://www.arng.army.mil/about_us/ai ding_america.asp> [31 January 2003].

Bush, George W. National Strategy to Combat Weapons of Mass Destruction: 17 September 2002.

Clinton, William J. A National Securtiy Strategy for a Gloabal Age. The White House. Washington, DC: December 2000.

"The Department of Homeland Security." The White House Home Page. <http://www.whitehouse.gov/deptofhomeland/> [24 January 2003].

Grohoski, David C. The Vulnerabilities of US Strategic Ports to Acts of Sabotage. Unpublished Research Paper, U.S. naval War Command and Staff College, Newport, RI: 12 February 1996.

"Homeland Defense." U.S. Northern Command Homepage. <http://www.northcom.mil/index.cmf?fuseaction=s.homeland> [20 December 2002].

Iraq's Weapons of Mass Destruction. Central Intelligence Agency: October 2002.

Landry, Mary. <MLandry@MSOProv.uscg.mil> "Capt of the Port Info." [E-mail to Anthony Calandra <calandra@nwc.navy.mil>] 27 January 2003.

Lofgren, Mike. "Measuring the Costs of the War Against Terrorism." The Budget Monitor. 19 June 2002. Vol. 2, No. 6. <http://www.budget.house.gov/budmon2006.pdf> [18 January 2003].

Loy, James M. "Protecting the Homeland: U.S. Coast Guard." Power Point presentation to Governor Ridge. 28 September 2001.

Matthews, James K. "United States Transportation Command: A Short History." United States Transportation Command Homepage. 25 October 2002. <http://public.transcom.mil/history.html> [19 December 2002].

Mineta, Norman and James M. Loy. The Subcommittee on Coast Guard and Maritime Transportation Hearing on Port Security. 06 December 2001. <http://www.house.gov/transportation/cgmt/12-06-01/12-06-01memo.html> [20 December 2002].

"Morehead City Sea Port of Embarkation, Morehead City, NC." Global Security Organization Homepage. 24 June 2002. <http://www.globalsecurtiy.org/military/facility/morehead-city.htm.> [31 January 2003].

"MTMC, About Us." Military Traffic Management Command Homepage. <http://www.mtmc.army.mil/> [19 December 2002].

Murray, James. <JFMurray@gruwoodshole.uscg.mil> "Port Security Paper for JWC Student." [E-mail to Anthony Calandra <calandra@nwc.navy.mil>] 23 January 2003.

Murray, James. U.S. Coast Guard Group Commander.. Telephone conversation, 22 January 2003.

Nash, William P. America's Commercial Seaports: An Achilles Heel. Unpublished Research Paper, Council on foreign Relations: 18 June 2001.

Office of Homeland Security. The National Strategy for Homeland Security. Washington, DC: 16 July, 2002.

Office of Naval Intelligence and U.S. Coast Guard Intelligence Coordination Center. Threats and Challenges to Maritime Security 2020. Washington, DC: 01 March 1999.

Olson, Greg D. Operational Concerns of Decontamination in Mitigating the Effects of Chemical and Biological Weaons Against Sea Ports. Unpublished Research Paper, U.S. Naval War Command and Staff College. Newport, RI: 13 May 2002.

Payne, Keith B. "Deterring the Use of Weapons of Mass Destruction: Lessons from History." United Kingdom. Comparative Strategy. Vol. 14: October 1995. 347-359.

Ross, Scott D. <USTCPA@hq.transcom.mil> "Chem/Bio Security for Ports of Embarkation." [E-mail to Anthony Calandra <calandra@nwc.navy.mil>] 03 January 2003.

Sidell, Frederick, Ernest T. Takafuji and David R. Franz. Medical Aspects of Chemical and Biological Warfare. Borden Institute, Walter Reed Army Medical Center. Washington, DC: 1997.

"United States Transportation Command Mission." USTRANSCOM Mission Statements. <http://public.transcom.mil/missions/mission.html> [19 December 2002].

U.S. Army Department. NBC Decontamination. FM 3-5. Washington, DC: 28 July 2000.

U.S. Department of Defense. Chemical and Biological Defense Program. Volume I. Annual Report to Congress: April 2002.

U.S. General Accounting Office. Subcommittee on National Security. Veterans Affairs, and International Relations House Committee on Government Reform. Port Security, Nation Faces Formidable Challenges in making New Initiatives Successful. GAO-02-993T: 05 August 2002.

U.S. Joint Chiefs of Staff. Joint Tactics, Techniques, and Procedures for Transportation Terminal Operations. Joint Pub 4-01.5. Washington, DC: 09 April 2002.

U.S. Transportation Command. Understanding the Defense Transportation System. "USTRANSCOM Handbook 24-2 Third Edition." Washington DC: 01 September 2000.

"Who We Are -- Mission." U.S. Northern Command Homepage. <http://www.northcom.mil/index.cfm?fuseaction=s.whoweare&section=3> [20 December 2002].

World Heath Organization Communicable disease Surveillance and Response (CSR). Frequently Asked Questions Regarding the Deliberate Use of Biological Agents and Chemicals as Weapons. 2001. <http://www.who.int/emc/questions.htm.> [19 December 2002].